## REMARKS

Initially, Applicant notes that the remarks and amendments made by this paper are consistent with the proposals presented to the Examiner during the telephone call of May 15 2007.

By this response, claims 1, 3-6, 8-9, 15, 17, 19, and 24 have been amended[1] and no claims have been added or cancelled, such that claims 1-28 remain pending, of which claims 1, 5, 9, and 19 are the only independent claims at issue.

The Non-Final Office Action, mailed May 7, 2007, considered and rejected claims 1-28. Claims 1, 3-4, 6, 8-9, 15, 17 and 24 were objected to because of minor informalities. Claims 1-9, 11-12 and 19 were rejected to under 35 U.S.C. § 103(a) as being unpatentable over Jerdoneck (US 6,983,381 B2), hereinafter Jerdoneck. Claims 10, 13, 16, 18, 20, and 23-28 were rejected under 35 U.S.C. § 103(a) as being unpatentatble over Jerdoneck (US 6,983,381 B2) in view of Salgarelli et al. (EAP-Shared Key Exchange (EAP-SKE): A scheme for Authentication and Dynamic Key Exchange in 802.1X Networks, April 30, 2002).[2]

Applicant's claimed invention is generally directed to embodiments for efficiently and securely authenticating computer systems. The embodiment of claim 1, for example recites a method for receiving credentials in a client computing system that can be used to can authentic with a server computing system. The method initially includes an act of receiving a limited use credential. A secure link between the client computing system and the server computing system is then established. The limited-use credential is then submitted to the server computing system over the established secure link. In response to submitting the limited-use credential, the client receives an additional credential from the server computing system over the established secure link. The additional credential can be used for subsequent authentication with the server computing system and is provisioned at the server computing system based on the limited-use credential.

---

[1] Support for the claim amendments is found in the claims as originally written as the amendment merely clarify limitations that were already inherent in the claims. Further support can be found throughout the specification including, but not limited to, the disclosure found in ¶¶ [0013], [0014], [0039], and [0048].

[2] Although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

The methods recited in claims 1 and 5 are similar, but whereas claim 1 is recited from the perspective of a client computing system, claim 5 is recited from the perspective of a server computing system interacting with the client computing system.

The only other independent claims, 9 and 19, are generally directed to embodiments for efficiently and securely authenticating computer systems, but they differ in their approach as compared to claims 1 and 5. While claims 1 and 5 are generally directed to utilizing a limited use credential for authentication, claims 9 and 19 are generally directed to a method for facilitating the negotiating authentication mechanisms from among a number of different authentication mechanisms. Claim 9 recites the method from a client's perspective, while claim 19 recites the method from the perspective of a server computing device. For instance, claim 9 recites a method for participating in authentication with a server computing system. The method includes receiving a first server request that includes at least a first indication of the authentication mechanisms deployed at the server computing system. A response is sent to the first server request that includes at least a second indication of the authentication mechanisms deployed at both the client computing system and the authentication mechanisms deployed at the server computing system. A tunnel key is then identified that can be used to encrypt content transferred between the client computing system and the server computing system. A second server request that includes encrypted authentication content is received, the encrypted authentication content being encrypted with the tunnel key. The encrypted authentication content is decrypted with the tunnel key to reveal unencrypted authentication content. The unencrypted authentication content indicates a mutually deployed authentication mechanism that both the client computing system and the server computing system support. A second response is then sent, the second response including encrypted response data that is responsive to the unencrypted authentication content. The encrypted response data is utilized for authenticating with the server computing system according to the mutually deployed authentication mechanism.

Initially, it will be noted that all of the independent claims were rejected in view of a single reference, namely Jerdoneck. Jerdoneck is generally directed to embodiments for pre-authentication of users in a network computing system using one-time passwords. In Jerdoneck, a client requests a one time password, a server generates an inactive one time password and then

the one time password is communicated to the client. The user is then authenticated at which time the one time password is authenticated.

While the cited art of Jerdoneck is generally directed to client authentication, Applicant respectfully submits that many of the limitations required in the independent claims fail to appear, or be suggested by the cited art. For example, with regard to independent claims 1 and 5, Jerdoneck fails to teach or suggest, among other things, that the additional credential is provided over the established secure link in response to the client submitting the limited use credential. In the office action, col. 5, ll. 53-56, col.8 ll. 60-65, and col. 3, ll. 50-53 of Jerdonek are relied upon as demonstrating the limitation of an act of receiving an additional credential that can be used for subsequent authentication with the server computing system. However, the cited paragraphs disclose a credential that is received prior to the user submitting the limited-use credential. Therefore, the additional credential is not being received **in response to submitting the limited use credential**, as recited in the claims, together with the other limitations. For at least this reason, the Jerdonek does not anticipate the embodiments of independent claims 1 and 5.

With regards to independent claims 9 and 19, it will be noted that the same reference of Jerdoneck was used to reject the claims. The embodiment of claims 9 and 19 are generally directed to solving a problem that Jerdoneck fails to even address and accordingly contains limitations not present in Jerdoneck. The embodiments recited in claims 9 and 19 facilitate the negotiation of authentication mechanisms from among a number of different authentication mechanisms. When the claims address receiving a server request that includes at least the authentication mechanisms deployed at the server computing system, they are not indicating that the authentication mechanism is being utilized in the request, but rather that supported authentication mechanisms are being indicated as the computing systems negotiate an authentication mechanism to utilize. The references cited by the Examiner as purportedly including this limitation, each disclose only that an authentication mechanism is being used, not that the available authentication methods available to a computing system are being indicated to the other computing system. The cited art fails to teach or suggest communicating the available authentication methods because the cited art is not negotiating an authentication method; it is merely implementing a predetermined method. For at least the reason that the Jerdoneck does

not teach or suggest actually indicating the actual authentication mechanisms available at each computing device, Jerdoneck does not anticipate the embodiments of claims 9 and 19.

In view of the foregoing, Applicant respectfully submits that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice. Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at 801-533-9800.

Dated this 7th day of August, 2007.

Respectfully submitted,

RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
JOHN C. BACOCH
Registration No. 59,890
Attorneys for Applicant
Customer No. 47973

JCJ:ahy
AHY0000005106V001